Reproducibility, trust, and proof checkings

Dale Miller, Inria Sacla

Formal proofs are produced and checked by machines. Machines are physical devices, of course, and their software and their execution are subject to errors. As in other scientific domains, reproducibility is key to establishing trust, whether it is a claim in physics or a claim that a given file contains a valid proof. A high degree of trust in a formal proof comes from executing a trusted proof checker on a claimed proof, thereby, reproducing the claim. In order to trust a proof checker, it should be possible to implement new proof checkers or to exam the source of existing provers and to be convinced that they are sound implementations of logic. Providing a formal semantics for proof languages is an important step in allowing for this kind of independent and trustworthy proof checking to be achieved.